mod p^2 で p乗剰余になっている数の分布について(数論の学際的研究)

AUTHOR(S):

村田, 玲音

CITATION:

村田, 玲音. mod p^2 で p乗剰余になっている数の分布について(数論の学際的研究). 数理解析研究所講究録 1993, 837: 122-129

ISSUE DATE:

1993-05

URL:

http://hdl.handle.net/2433/83490

数理解析研究所講究録
837巻 1993年 122-129

mod p^2 で p 乗剰余になっている数の分布について

村田　玲音 (Leo MURATA)
明治学院大学　一般教育部

1.　問題の説明

p を奇素数、Z_p を p進整数環とする。多項式　$X^{p-1}-1$　を　$Z_p[X]$ で因数分解すると、1次式 p−1 個の積になることが知られている。こうして得られた p−1 個の1の p−1 乗根を $\alpha_1, \ldots, \alpha_{p-1}$ としよう。これらは p進整数なのでそれぞれ Hensel 展開できるが、α_i の2番目の Hensel係数を a_i とする。

ここでは　$\{ a_i ; 1 \leqq i \leqq p-1 \}$ がどんな分布をしているのか、それを考えたい。

これらは Hensel係数なので 0 以上 p−1 以下の自然数であるが、区間 [0, p−1] のどこかにかたまって分布しているとは考えにくい。これらは均一に分布していると考える方が自然に思えるが、それを証明することはできるのだろうか。

この問題を考える前段階として、α_i の最初の Hensel係数の分布を見てみよう。すると、ここには1から p−1 までの値が丁度1回づつ現われることが容易に分かる (Fermat の小定理による)。従って「最初の Hensel係数の分布関数」を作ってみると図1のようになってしまう。縦横の長さが全ての素数に対して1となるように"規格化"すると図2のようになる。ここで素数 p を∞に大きくしてゆくと、この分布関数は図3のように、一定の線分に近づく。これが「最初の Hensel係数はほぼ均一に分布している」ことの一つの解析的な表現である。しかも「Hensel係数はほぼ均一に分布しているだろう」という直感が正しかったことを、最初の Hensel係数の場合には完全に証明できたわけである。

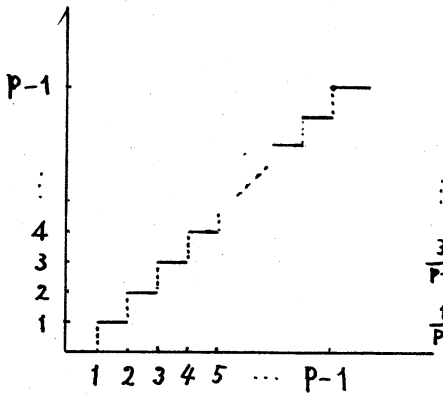

図1

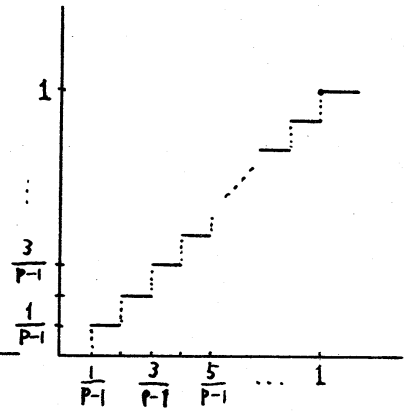

図2

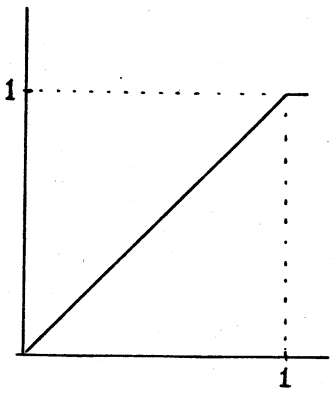

図3

これを参考にして「二番目の Hensel係数の分布」を調べたいのだが、その前に何故こうした問題を考えるのか、その背景に触れておこう。

2. 問題の背景

I. 原始根に関する Artin予想との関係

b は素数 p で割れない自然数とし、i も自然数とする。次の定義を置く：

$[(Z/p^iZ)^*:\langle b(\mathrm{mod}\ p^i)\rangle] = r(b,p^i)$, p^iを法とする b の剰余指数。

ただし、$(Z/p^iZ)^*$ は mod p^i の既約剰余類群、＜＊＞は＊の類が作る乗法的部分群、［：］は部分群の指数を表す。

i＝1 の時、b を固定して b を原始根に持つような素数 p がどのように分布しているかを考察する問題が、「原始根に関する Artinの予想」である。そしてこの予想については、現在までにかなり色々なことが分かってきた。ところが、i≧2 の場合は何一つ分かっていないといってもよい状態である。そこで、b (mod p) が原始根に

なっているとき、この類を mod p^2 で考えたらどうなるか？　といったことを考えてみよう。

類 $b(\mathrm{mod}\ p^i)$ を mod p^{i+1} で考えると、

$$b(\mathrm{mod}\ p^{i+1}),\ b+p^i(\mathrm{mod}\ p^{i+1}),\ \ldots,\ b+(p-1)p^i(\mathrm{mod}\ p^{i+1})$$

と $p-1$ 個の類に分裂してしまう。その際、次の二つの補題が成立する：

補題 1　　$r(b,p^i)=n$ なら、分裂した全ての類について $r(b+kp^i,p^{i+1})=n$ or np.

補題 2　　$r(b,p^i)=n$ とする。

① $(Z/p^iZ)^*$ における b の類の位数が p で割れるなら、分裂した全ての類で $r(b+kp^i,p^{i+1})=n$.

② この b の類の位数が p で割れないなら、分裂した p個の類のうち、ある一つの K のみに対して $r(b+Kp^i,p^{i+1})=np$ が起こり、残りの類については n のままである。

一例として、ある b が p を法として原始根になっている場合を考えよう。
$b\ (\mathrm{mod}\ p)$ という類の挙動を、mod p^2, mod p^3, ... とべきを上げて行きながら観察すると、常に指数が $p-1$ になっているような類の列

$$b(\mathrm{mod}\ p),\quad b+kp(\mathrm{mod}\ p^2),\ b+kp+hp^2(\mathrm{mod}\ p^3),\ \ldots$$

を考えることができる。これから得られる数列 : b, b+kp, $b+kp+hp^2$, ... によって定まる p進整数が先程の α に他ならない。この例では数列が b から始まっているので、α_b が現われている。

このように考えると、次の事は明らかである：

{ p : b が mod p^2 で原始根 }

= { p : b が mod p で原始根 } − { p : b が mod p^2 で丁度 p乗剰余 } .

そして右辺第１項は Artin予想の研究によってかなり分かっており、右辺第２項は「α_bの２番目の Hensel係数＝0 であるような素数」を数えることによって、上からの評価を得ることができる。こうして、２番目の Hensel係数の分布を知る必要がでてきた。

Ⅱ. Fermat's Last Theorem Case 1 との関係

次の定理はよく知られている：

Theorem (Wieferich et al) 100 以下のある素数 q に対して $q^{p-1} \not\equiv 1 \pmod{p^2}$ が成立するなら、この素数 p に対して Fermatの大定理の第一の場合は正しい。

容易に分かるように、上の定理に現われた合同式は「$r(q, p^2)$ が p で割れ(ない)」という条件と同値になり、更に上の補題によれば「$a_q \not\equiv 0$」と同値になる。従って、やはり２番目の Hensel係数が問題になった。

3. これまでに得られたこと

以下では素数 p を固定する。$\{ a_i \}_{i=1}^{p-1}$ の分布を調べるために、第一の Hensel係数の場合の考察を参考にし、まず分布関数を定義しよう。実変数θに対し、

$$f_p^+(\theta) = (p-1)^{-1} \#\{ i ; 1 \leqq i \leqq p-1, a_i \leqq \theta (p-1) \},$$

$$f_p^-(\theta) = (p-1)^{-1} \#\{ i ; 1 \leqq i \leqq p-1, a_i < \theta (p-1) \},$$

とおき、これの相加平均 $f_p(\theta)$ を $\{a_i\}$ の分布関数とする。

これが次の性質を持つことは、定義から明らかである：

① 実質的には、階段関数である。

② 単調非減少関数である。

③ $\theta<0$ なら $f_p(\theta)=0$, $\theta>1$ なら $f_p(\theta)=1$ になる。

そして、先程の我々の予想を定式化すると次のようになるだろう：

予想 $\lim_{p\to\infty} f_p(\theta)=\theta$? ただし $0\leqq\theta\leqq1$.

これについて現在証明出来ていることは、次の二点である：

定理1

$$\int_0^1 f_p(\theta)\,d\theta = \frac{1}{2} .$$

定理2

$$f_p\left(\frac{1}{2}\right) = \frac{1}{2} .$$

定理1によれば、我々の予想は"平均的な意味で"正しい。又、定理2によれば、$\theta=1/2$ では成り立っていることも証明できた。この他にも、確率的考察や数値例など、予想を支持する事実はいくつかあるのだが、一方これを証明することはかなり困難であることも分かってきた。以下に書くように、上の予想は解析数論における幾つ

かの重要な問題とほとんど同値になっており、それらの同値な命題を見るとその困難さが理解できるのである。

4. 上の予想とほとんど同値な他の命題

① 指標和との関係

mod p^2 の Dirichlet指標のうち、$\chi^p = \chi_0$, $\chi \neq \chi_0$ を満たすものの集合をKとおく。ここで、χ_0 は勿論 principal character を表す。

Proposition 1. 次の評価式と我々の予想は同値である。ただし N は任意の自然数。

$$\frac{1}{p} \sum_{\chi \in K} \sum_{n=1}^{N} \chi(n) \ll p \cdot o(1).$$

指標和に関する Pólya-Vinogradov の有名な不等式を使うと、上の式の右辺として $p(\log p)$ を取ることができる。又、一般リーマン予想の仮定のもとで得られた指標和の評価を使うと、この右辺は $p(\log\log p)$ と改良できる。上の Proposition は、この $(\log p)$ あるいは $(\log\log p)$ の部分を $o(1)$ まで良くできるかどうかを問題にしているわけだが、色々な事情から考えて、この改良はかなり難しいと思われる。

② Heilbronnの問題との関係

『$\sum_{a=1}^{p-1} \exp(2\pi i a^p p^{-2})$ に対して non-trivial な評価を求めよ』という問題がある(Heilbronnの問題)。ここで non-trivialな評価とは $o(p)$ のことであるが、これはまだ解決されていない。

実は、この問題も我々の予想と深い関係がある。

Proposition 2. I) $\sum_{a=1}^{p-1} \exp(2\pi i n a^p p^{-2}) = o(p(\log p)^{-1})$ が $p-1$ 以下のすべての n で正しいならば我々の予想は正しい。

II) 逆に、我々の予想が正しければ、Heilbronnの問題は $o(p)$ の形で解ける。

③ Gauss和の偏角分布との関連

指標 χ の Gauss和を $G(\chi)$ と書くことにすると、次が成立する：

Proposition 3. 次の式が正しいなら我々の予想も正しい：

$$\lim_{p\to\infty} (\log p) \sum_{\chi\in K} \frac{G(\chi)}{p} = 0 .$$

この式のΣ記号の中は、Gauss和の偏角であるから、Kに属する指標の偏角がほぼ均一に分布していることと、我々の予想は関係がある。

色々な面から考えて、私は我々の予想は正しいだろうと考えているが、上述のようなわけでその証明は相当難しそうである。私としては「指標和の評価」を使って予想を証明するのが一番有望だろうと思っているが確信はない。ただ、このように見てくると mod p^2 の場合には様々な問題が関係していて非常に面白い。今後の研究が待たれるところである。

参考文献

[1] C. Hooley : On Artin's Conjecture. J. f. reine u. angew. Math. Vol.225 (1967), p.p. 209-220.

[2] P. Riebenboim : "13 Lectures on Fermat's Last Theorem", Springer 1979.

[3] H.L. Montgomery-R.C. Vaughan : Exponential sums with multiplicative Coefficients, Invent. Math. Vol.43 (1977), p.p. 69-82.

[4] W.L.Fouche : Arithmetic properties of Heilbronn sums, J. of Number Theory Vol.19 (1984), p.p. 1-6.

[5] L. Murata : Some remarks on the distribution of numbers which are p-th power residue mod p^2, (pre-print).

１９９３年２月　記